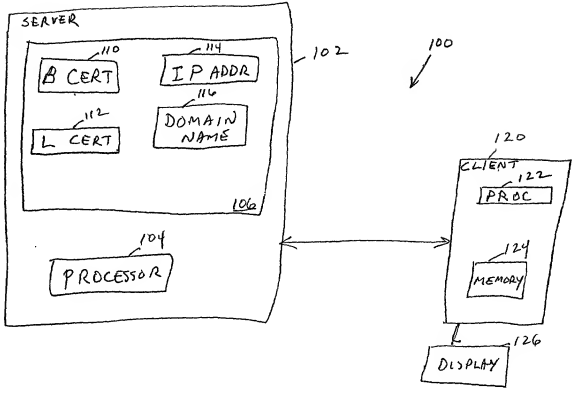
SERVER
110
B CERT
114
IP ADDR
116
DOMAIN NAME
112
L CERT
102
100
106
104
PROCESSOR
120
CLIENT
122
PROC
124
MEMORY
126
DISPLAY

FIG. 1

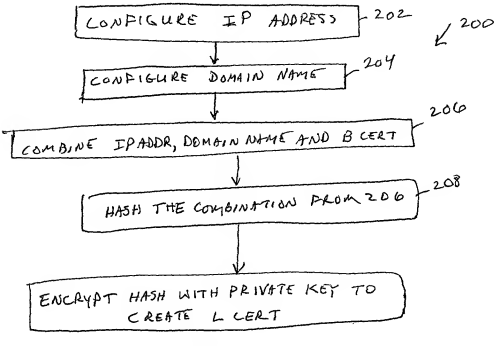
CONFIGURE IP ADDRESS
202
200
CONFIGURE DOMAIN NAME
204
COMBINE IPADDR, DOMAIN NAME AND B CERT
206
HASH THE COMBINATION FROM 206
208
ENCRYPT HASH WITH PRIVATE KEY TO CREATE L CERT

FIG. 2

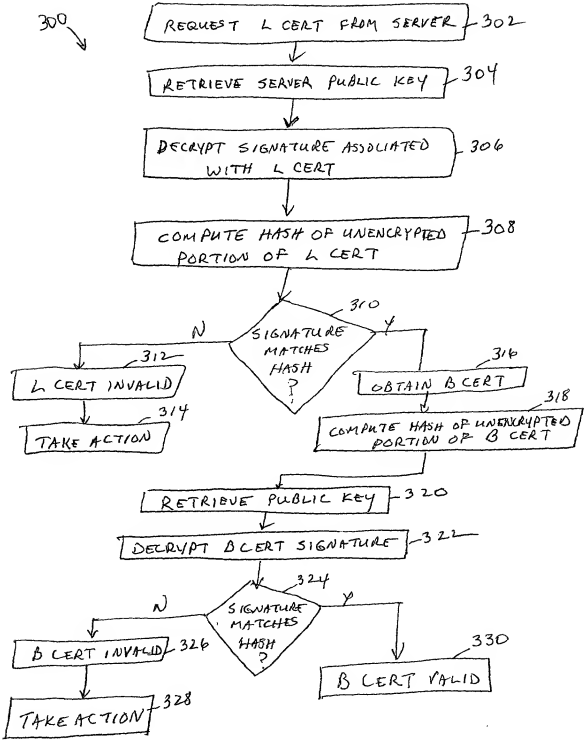
300
REQUEST L CERT FROM SERVER
302
RETRIEVE SERVER PUBLIC KEY
304
DECRYPT SIGNATURE ASSOCIATED WITH L CERT
306
COMPUTE HASH OF UNENCRYPTED PORTION OF L CERT
308
310
SIGNATURE MATCHES HASH ?
N
Y
312
L CERT INVALID
314
TAKE ACTION
316
OBTAIN B CERT
318
COMPUTE HASH OF UNENCRYPTED PORTION OF B CERT
RETRIEVE PUBLIC KEY
320
DECRYPT B CERT SIGNATURE
322
324
SIGNATURE MATCHES HASH ?
N
Y
B CERT INVALID
326
TAKE ACTION
328
330
B CERT VALID

FIG. 3